LastPass •••|

Psychologie des mots de passe

Expansion de la vie connectée et (mauvais) comportements en matière de mots de passe

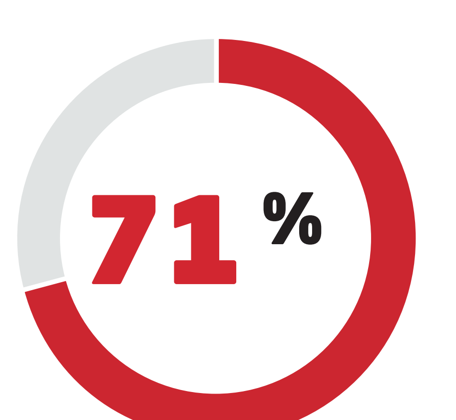


Sécurité des mots de passe en 2021 : déjouer les vulnérabilités humaines

La pandémie de COVID-19 a bouleversé les lieux de travail de millions de personnes dans le monde. Fermeture des bureaux physiques. Nombreux sont ceux qui sont passés au travail à domicile. Avec nulle part où aller, ils ont passé plus de temps en ligne.

Les individus comme les entreprises sont plus que jamais en danger. Les pirates tirent parti et exploitent plus que jamais les vulnérabilités humaines. Les types d'attaques ont évolué pour exploiter le grand nombre de personnes qui télétravaillent et qui passent davantage de temps en ligne.

Pendant la pandémie :



ont télétravaillé à temps partiel ou à plein temps.



ont passé plus de temps en ligne pour se divertir et pour travailler.

Selon le rapport DBIR (Data Breach Investigations Report) de 2021, les cybercriminels ciblent de plus en plus les particuliers et leurs appareils.

85 %

Un nombre impressionnant de fuites de données, 85 %, impliquent un élément humain (hameçonnage, vol d'identifiants ou erreur humaine).

36 %

36 % des fuites l'année dernière étaient associées à l'hameçonnage, en augmentation de 11 %.

Présentation de l'étude

Notre rapport Psychologie des mots de passe étudie les comportements en matière de sécurité des mots de passe de 3 750 professionnels de sept pays. Nous avons interrogé les répondants sur leurs sentiments et comportements en matière de sécurité en ligne.

Pays étudiés :

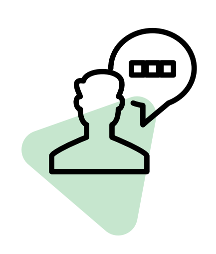
- États-Unis
- Royaume-Uni
- Allemagne
- France
- Australie
- Singapour
- Inde



Sensibilisation élevée, actions insuffisantes

Ce que les gens disent.

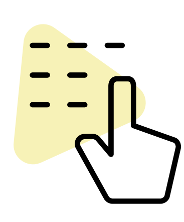
79 %
pensent que le piratage des mots de passe est préoccupant...



Ce que les gens font.

51 %
...confient à leur mémoire la gestion des mots de passe.

92 %
savent que réutiliser le même mot de passe ou presque est une pratique risquée...



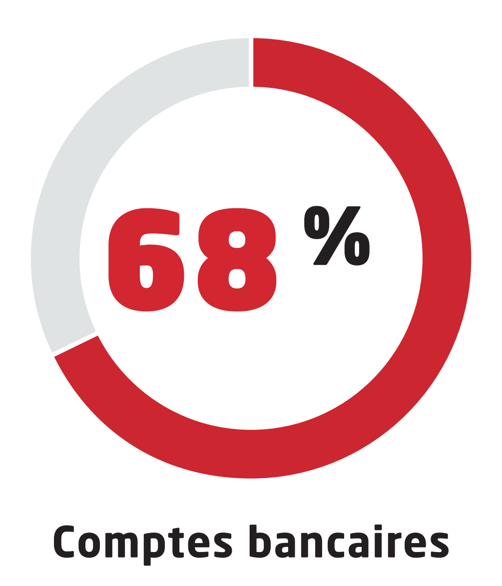
65 %
...utilisent toujours ou presque toujours le même mot de passe ou une variante.



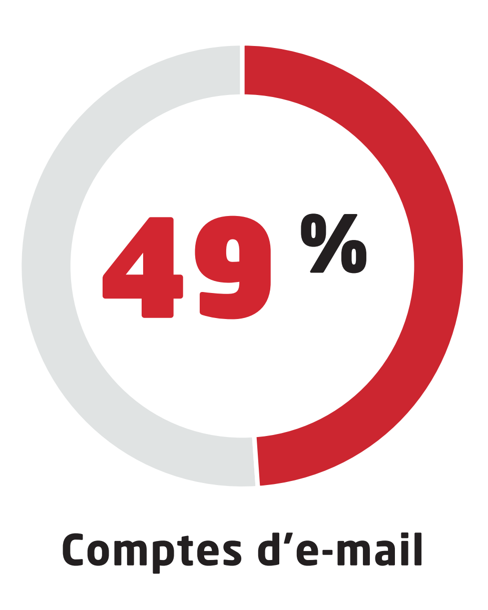
45 % N'ONT PAS MODIFIÉ LEURS MOTS DE PASSE

45 % des personnes interrogées n'ont pas modifié leurs mots de passe au cours de l'année écoulée, y compris après une fuite de données.

Les gens appliquent une sécurité sélective aux mots de passe, mais créeraient des mots de passe plus forts pour :



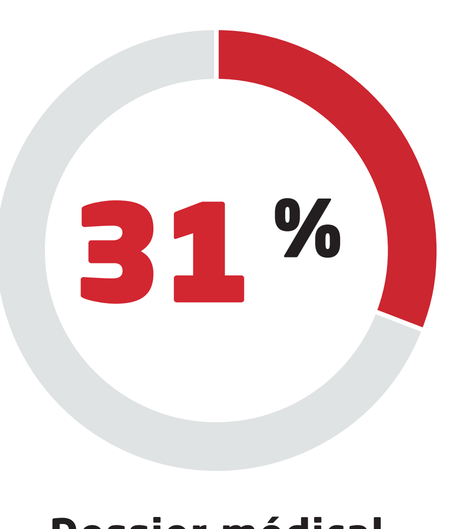
Comptes bancaires



Comptes d'e-mail



Comptes professionnels



Dossier médical



8 %

8 % seulement disent qu'un mot de passe fort ne doit pas faire référence à des informations personnelles.

Ce qui signifie que la plupart des utilisateurs créent des mots de passe basés sur des informations personnelles potentiellement associées à des données publiques, comme la date de naissance ou l'adresse privée.

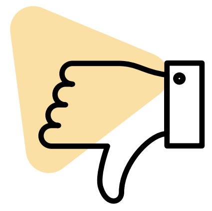


CONSEIL DE PRO

Utilisez des phrases dénuées de sens parsemées de chiffres et de symboles plutôt que des mots individuels afin de rendre vos mots de passe plus longs, plus forts et plus simples à mémoriser, tout en les rendant plus durs à deviner pour les pirates.

Angles morts et points forts

La dissonance cognitive prédomine. Les gens piochent les informations qu'ils jugent dignes d'être protégées. Par conséquent, ils adoptent sciemment des comportements risqués en matière de mots de passe, alors même qu'ils passent un temps record en ligne pour le travail et le divertissement durant la pandémie.



83 % ne sauraient pas si leurs données étaient disponibles sur le dark web.



76 % déclarent utiliser la MFA tant pour des raisons personnelles que professionnelles, une augmentation de 10 % en un an.



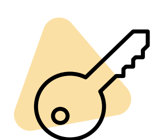


CONSEIL DE PRO

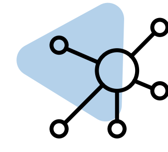
Traitez tous les identifiants comme des données vulnérables. Vous pensez peut-être que les identifiants de votre salle de sport n'ont aucune valeur pour les pirates, mais si ces identifiants sont identiques ou proches de ceux que vous utilisez pour consulter vos comptes bancaires, une fuite de données de votre salle de sport peut potentiellement exposer des données financières sensibles.

Expansion de la vie connectée

Plus de comptes que jamais.



91 % des sondés ont créé un compte cette année.



90 % des sondés déclarent posséder jusqu'à 50 comptes en ligne/d'applications.

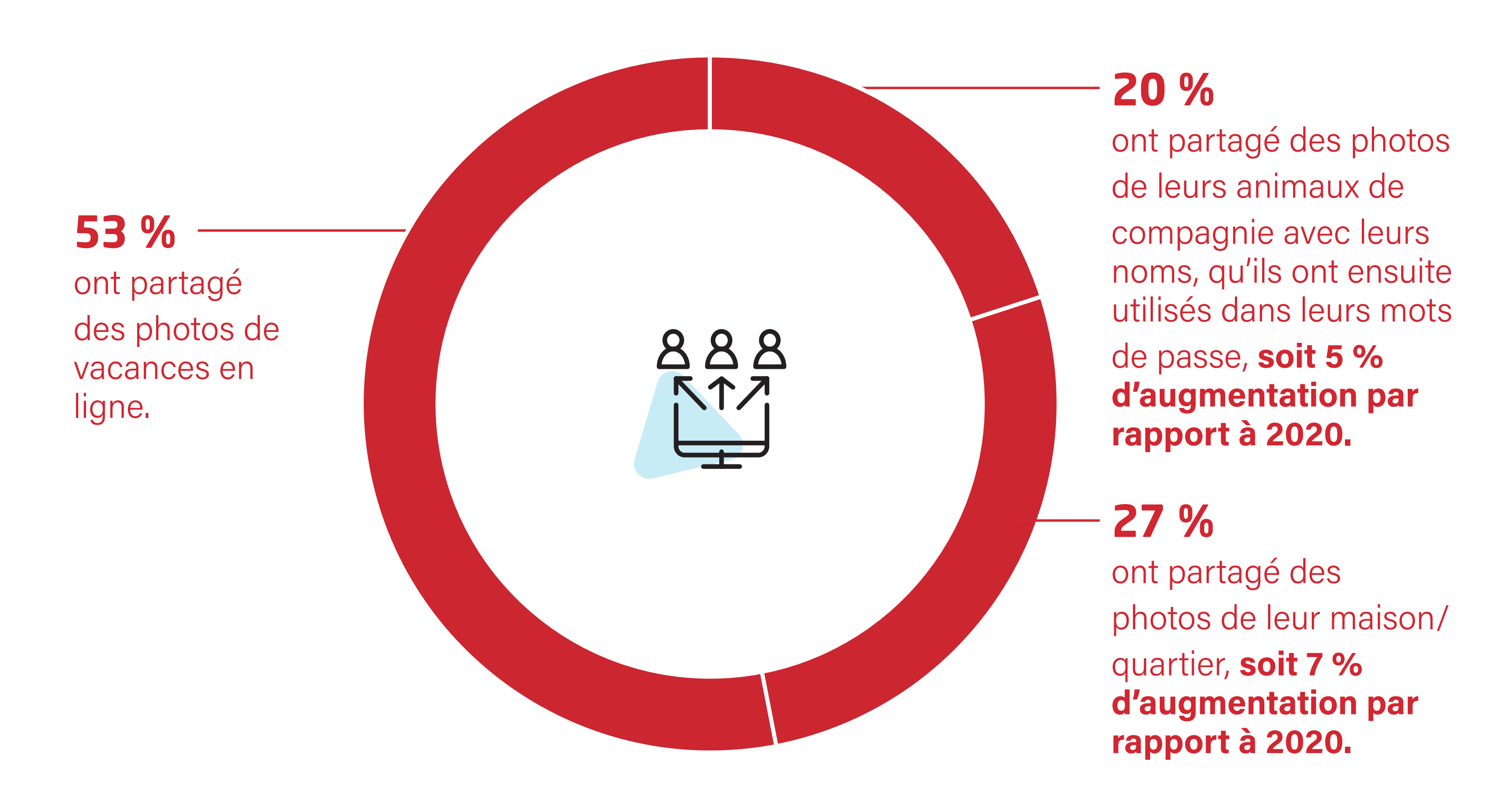
50 %

Les répondants ont 50 % de comptes en plus en 2021 qu'en 2020.

Plus notre présence numérique se développe, plus la protection de nos données personnelles doit être renforcée.

Notre vie connectée a connu une forte expansion durant la pandémie de COVID-19. La déconnexion de notre vie quotidienne nous a plus que jamais incités à nous connecter en ligne. Le résultat : plus de nouveaux comptes, et plus de données personnelles partagées en ligne.

La quantité de données personnelles en ligne augmente :





CONSEIL DE PRO

Passez vos comptes sur les réseaux sociaux en privé, ou soyez avare de publications publiques. Des acteurs malveillants parcourent les profils publics pour tenter d'exploiter des données qui peuvent sembler inoffensives pour pirater des comptes en dehors des réseaux sociaux.

Télétravail : le point de vue des employés et des employeurs.



Employé
habitudes de télétravail :

47 % n'ont pas modifié leurs comportements de sécurité en ligne depuis le passage au télétravail.

46 % n'ont pas renforcé leurs mots de passe en télétravail.

44 % ont partagé des informations et des mots de passe de comptes professionnels en télétravail.

Employeur
habitudes de télétravail :

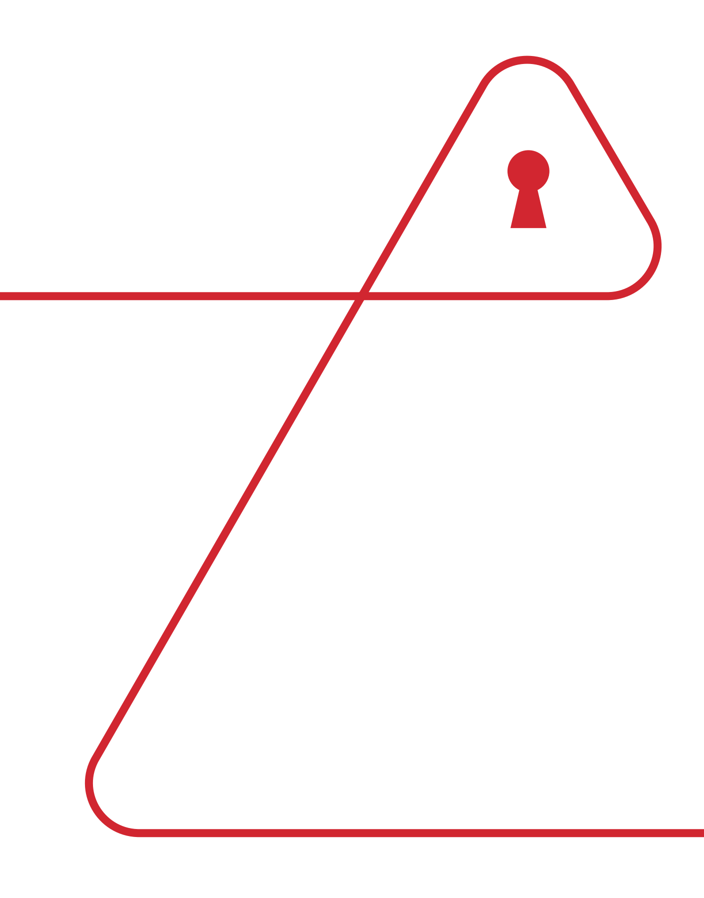
39 % se sont assuré que chaque employé en télétravail se connecte au réseau de l'entreprise via des réseaux sécurisés.

35 % ont obligé les employés à changer leurs mots de passe plus régulièrement.

35 % ont renforcé les méthodes d'authentification.

Les administrateurs informatiques doivent faire attention. L'existence du risque n'incite pas en soi les gens à adopter des comportements plus sûrs. Près de la moitié des employés en télétravail adoptent des comportements à risque en matière de mots de passe.

Les administrateurs informatiques doivent repenser leurs stratégies de sécurité de la même manière que les employés doivent s'adapter à de nouvelles façons de travailler.





CONSEIL DE PRO

Investissez dans une solution de **gestion des mots de passe** pour améliorer l'hygiène et la sécurité des mots de passe. Mettez en œuvre le **SSO** et la **MFA** pour sécuriser tous les points d'accès. Organisez des formations sur la sécurité pour éduquer et évangéliser.

Instantané régional :

Royaume-Uni



61 % savent qu'un mot de passe fort et unique ne doit pas faire référence à des informations personnelles.

Ils sont aussi les moins susceptibles de partager des informations personnelles en ligne **(41 %).**

Allemagne



L'Allemagne est en tête pour ce qui est de la connaissance du dark web **(79 %).**

Seuls **14 %** d'entre eux sauraient si leurs informations personnelles se retrouvaient sur le dark web.

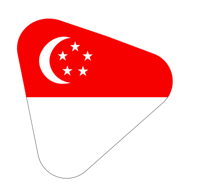
France



Seuls **15 %** des répondants Français ont télétravaillé durant le COVID.

Ils ne sont que **43 %** à avoir modifié leurs comportements en matière de sécurité en ligne en cas de télétravail.

Singapour



Les répondants de Singapour sont les plus préoccupés par le piratage des mots de passe **(93 %).**

Ils sont également en tête lorsqu'il s'agit de savoir quoi faire s'ils sont piratés **(74 %).**

Inde



L'Inde est nettement plus susceptible d'utiliser un gestionnaire de mots de passe ou un navigateur pour stocker les mots de passe que les autres pays **(64 %).**

Les répondants indiens sont en tête lorsqu'il s'agit de modifier les habitudes en matière de sécurité en ligne en télétravail **(81 %).**

Australie



71 % des Australiens utilisent toujours ou presque toujours le même mot de passe ou une variante.

Toutefois, les Australiens ont passé dans l'ensemble moins de temps en ligne durant la pandémie **(61 %).**

États-Unis



Les Américains sont plus susceptibles d'utiliser un service de surveillance du crédit si leur compte a été piraté **(31 %).**

Toutefois, **39 %** d'entre eux n'ont pas estimé nécessaire de modifier leurs habitudes en matière de sécurité en ligne en cas de télétravail, les jugeant déjà sûres.

Résumé de la situation

Pourquoi les gens adoptent-ils de mauvais comportements en matière de mots de passe (en toute connaissance de cause) ?

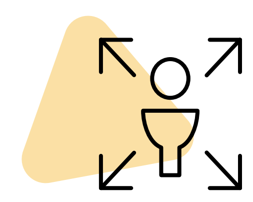
68 % de ceux qui réutilisent leurs mots de passe ont peur de les oublier.

52 % de ceux qui les réutilisent veulent garder le contrôle de leurs mots de passe.

36 % considèrent que leurs comptes ne présentent pas suffisamment d'intérêt pour les pirates.



Pourquoi la réutilisation des mots de passe est-elle si dangereuse, surtout en période d'expansion de nos vies connectées ?



Une seule combinaison de nom d'utilisateur et de mot de passe dérobée permet à un pirate d'accéder à de nombreux comptes.



Lorsqu'un cybercriminel obtient l'accès à un appareil utilisé à des fins personnelles et professionnelles, il peut accéder facilement au réseau de l'entreprise pour pirater des données ou détourner de l'argent.





LES GENS ONT DES MAUVAIS COMPORTEMENTS EN MATIÈRE DE MOTS DE PASSE

Avec des vies numériques en constante expansion et un manque d'assistance en matière de cybersécurité, une combinaison d'habitudes, d'émotions et de manque de sentiment d'urgence empêche les gens de modifier leurs comportements en ligne.

Lutter contre les mauvais comportements en matière de mots de passe

La pandémie de COVID-19 a entraîné un bouleversement sans précédent de nos modes de travail et d'interaction. Nous passons plus de temps en ligne. Nous partageons davantage en numérique. Puisque nous savons pourquoi les gens se comportent comme ils le font, comment faire pour corriger ces comportements ?

À quoi ressemble un bon comportement en matière de mots de passe ?

- Rendez chaque mot de passe unique.
- Utilisez des combinaisons de caractères dénuées de sens.
- Activez l'authentification à deux facteurs.
- Changez vos mots de passe en cas de fuite avérée.



Luttez contre la peur.

Utilisez un **gestionnaire de mots de passe** pour gérer et sécuriser vos mots de passe. Déléguez la création, la mémorisation et la saisie de vos mots de passe à un gestionnaire de mots de passe.

Luttez contre l'anxiété.

Ajoutez une couche de sécurité avec **l'authentification multifacteur (MFA)** pour être sûr d'être le seul à pouvoir accéder à vos informations.

Luttez contre l'apathie.

Surveillez vos données afin d'être sûr de savoir si vos informations ont été compromises, grâce à la **surveillance du dark web**.



LastPass •••|

Plus de 30 millions d'utilisateurs et 85 000 entreprises font confiance à LastPass pour stocker et remplir leurs mots de passe, leurs numéros de cartes bancaires et d'autres informations personnelles. Utilisez LastPass pour générer des mots de passe plus forts et pour les saisir automatiquement lorsque vous consultez des sites ou des applications, sur tous vos appareils.



En savoir plus